

# Sign-Rank Can Increase Under Intersection

Mark Bun

Simons Institute for the Theory of Computing, Berkeley, CA, USA  
Boston University, MA, USA

Nikhil S. Mande

Georgetown University, Washington, DC, USA

Justin Thaler

Georgetown University, Washington, DC, USA

## Abstract

The communication class  $\mathbf{UPP}^{\text{cc}}$  is a communication analog of the Turing Machine complexity class  $\mathbf{PP}$ . It is characterized by a matrix-analytic complexity measure called sign-rank (also called dimension complexity), and is essentially the most powerful communication class against which we know how to prove lower bounds.

For a communication problem  $f$ , let  $f \wedge f$  denote the function that evaluates  $f$  on two disjoint inputs and outputs the AND of the results. We exhibit a communication problem  $f$  with  $\mathbf{UPP}^{\text{cc}}(f) = O(\log n)$ , and  $\mathbf{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$ . This is the first result showing that  $\mathbf{UPP}$  communication complexity can increase by more than a constant factor under intersection. We view this as a first step toward showing that  $\mathbf{UPP}^{\text{cc}}$ , the class of problems with polylogarithmic-cost  $\mathbf{UPP}$  communication protocols, is not closed under intersection.

Our result shows that the function class consisting of intersections of two majorities on  $n$  bits has dimension complexity  $n^{\Omega(\log n)}$ . This matches an upper bound of (Klivans, O'Donnell, and Servedio, FOCS 2002), who used it to give a quasipolynomial time algorithm for PAC learning intersections of polylogarithmically many majorities. Hence, fundamentally new techniques will be needed to learn this class of functions in polynomial time.

**2012 ACM Subject Classification** Theory of computation  $\rightarrow$  Communication complexity; Theory of computation  $\rightarrow$  Boolean function learning

**Keywords and phrases** Sign rank, dimension complexity, communication complexity, learning theory

**Digital Object Identifier** 10.4230/LIPIcs.ICALP.2019.30

**Category** Track A: Algorithms, Complexity and Games

**Related Version** <https://eccc.weizmann.ac.il/report/2019/027/>

**Acknowledgements** Nikhil Mande and Justin Thaler were supported by NSF Grant CCF-1845125.

## 1 Introduction

The unbounded-error communication complexity model  $\mathbf{UPP}^{\text{cc}}$  was introduced by Paturi and Simon [21] as a natural communication analog of the Turing Machine complexity class  $\mathbf{PP}$ . In a  $\mathbf{UPP}^{\text{cc}}$  communication protocol for a Boolean function  $f(x, y)$ , there are two parties, one with input  $x$  and one with input  $y$ . The two parties engage in a private-coin randomized communication protocol, at the end of which they are required to output  $f(x, y)$  with probability strictly greater than  $1/2$ . The cost of the protocol is the number of bits exchanged by the two parties. As is standard, we use the notation  $\mathbf{UPP}^{\text{cc}}$  not only to denote the communication model, but also the class of functions solvable in the model by protocols of cost polylogarithmic in the size of the input.

Observe that success probability  $1/2$  can be achieved with no communication by random guessing, so the  $\mathbf{UPP}^{\text{cc}}$  model merely requires a strict improvement over this trivial solution.



© Mark Bun, Nikhil S. Mande, and Justin Thaler;  
licensed under Creative Commons License CC-BY

46th International Colloquium on Automata, Languages, and Programming (ICALP 2019).

Editors: Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi;

Article No. 30; pp. 30:1–30:14



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



Owing to this liberal acceptance criterion,  $\mathbf{UPP}^{\text{cc}}$  is a very powerful communication model, essentially the most powerful one against which we know how to prove lower bounds. In particular,  $\mathbf{UPP}^{\text{cc}}$  is powerful enough to simulate many other models of computing, and this makes  $\mathbf{UPP}^{\text{cc}}$  *lower bounds* highly useful. As one example, any function  $f(x, y)$  computable by a Threshold-of-Majority circuit of size  $s$  has  $\mathbf{UPP}^{\text{cc}}$  complexity at most  $O(\log s)$ , and this connection has been used to translate  $\mathbf{UPP}^{\text{cc}}$  lower bounds into state of the art lower bounds against threshold circuits (see, for example, [10, 22, 8, 28, 6]).

$\mathbf{UPP}^{\text{cc}}$  also happens to be characterized by a natural matrix-analytic complexity measure called *sign-rank* [21]. Here, the sign-rank of a matrix  $M \in \{-1, 1\}^{N \times N}$  is the minimum rank of a real matrix whose entries agree in sign with  $M$ . Equivalently,  $\text{sr}(M) := \min_A \text{rk}(A)$ , where the minimum is over all matrices  $A$  such that  $A_{i,j} \cdot M_{i,j} > 0$  for all  $i, j \in [N]$ . Paturi and Simon [21] showed the following tight connection between  $\mathbf{UPP}^{\text{cc}}$  and sign-rank: if we associate a function  $f(x, y)$  with the matrix  $M = [f(x, y)]_{x,y}$ , then the  $\mathbf{UPP}^{\text{cc}}$  communication complexity of  $f$  equals  $\log(\text{sr}(M)) \pm \Theta(1)$ .

While lower bounds on  $\mathbf{UPP}^{\text{cc}}$  complexity (equivalently, sign-rank) are useful in complexity theory, *upper bounds* on these quantities imply state of the art learning algorithms, including the fastest known algorithms for PAC learning DNFs and read-once formulas [17, 1]. More specifically, suppose we want to learn a concept class  $\mathcal{C}$  of functions mapping  $\{-1, 1\}^n$  to  $\{-1, 1\}$ .  $\mathcal{C}$  is naturally associated with a  $|\mathcal{C}| \times 2^n$  matrix  $M$ , whose  $i$ th row equals the truth table of the  $i$ th function in  $\mathcal{C}$ . Then  $\mathcal{C}$  can be distribution-independently PAC learned in time polynomial in the sign-rank of  $M$ . (The sign-rank of  $M$  is often referred to in the learning theory literature as the *dimension complexity* of  $\mathcal{C}$ .) Moreover, the resulting learning algorithm is robust to random classification noise, a property not satisfied by the handful of known PAC learning algorithms that are *not* based on dimension complexity.

For the purpose of our work, one particularly important application of the dimension-complexity approach to PAC learning was derived by Klivans et al. [16], who showed that the concept class consisting of intersections of 2 majority functions has dimension complexity at most  $\binom{n}{O(\log n)} \leq n^{O(\log n)}$ . They thereby obtained a quasipolynomial time algorithm for PAC learning intersections of two majority functions.<sup>1</sup> Prior to our work, it was consistent with current knowledge that the dimension complexity of this concept class is in fact  $\text{poly}(n)$ , which would yield a polynomial time PAC learning algorithm for intersections of constantly many majority functions.

## 1.1 Our Results

Despite considerable effort, progress on understanding sign-rank (equivalently,  $\mathbf{UPP}^{\text{cc}}$ ) has been slow. Our lack of knowledge is highlighted via the following well-known open question (cf. Göös et al. [13]). Throughout, for any function  $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$ ,  $f \wedge f$  denotes the function on twice as many inputs obtained by evaluating  $f$  on two disjoint inputs and outputting  $-1$  only if both copies of  $f$  evaluate to  $-1$ , i.e.,  $(f \wedge f)(x_1, x_2) := f(x_1) \wedge f(x_2)$ .

► **Question 1.** *Is the class  $\mathbf{UPP}^{\text{cc}}$  closed under intersection? In other words, suppose the function  $f(x, y): \{-1, 1\}^n \times \{-1, 1\}^n \rightarrow \{-1, 1\}$  satisfies  $\mathbf{UPP}^{\text{cc}}(f) = O((\log n)^c)$  for some constant  $c$ . Is there always some constant  $c_1$  (which may depend on  $c$ ) such that  $\mathbf{UPP}(f \wedge f) \leq O((\log n)^{c_1})$ ? More generally and informally, if  $\mathbf{UPP}^{\text{cc}}(f)$  is “small”, does this imply any non-trivial upper bound on  $\mathbf{UPP}^{\text{cc}}(f \wedge f)$ ?*

<sup>1</sup> In fact, their algorithm runs in quasipolynomial time for intersections of polylogarithmic many majorities.

Prior to our work, essentially nothing was known about Question 1. In particular, we are not aware of prior work ruling out the possibility that  $\mathbf{UPP}^{\text{cc}}(f \wedge f) \leq O(\mathbf{UPP}^{\text{cc}}(f))$ . On the other hand, for reasons that will become apparent in Section 1.2, there is good reason to suspect that there exists a function  $f$  with  $\mathbf{UPP}^{\text{cc}}(f) = O(\log n)$ , yet  $\mathbf{UPP}^{\text{cc}}(f \wedge f) \geq \Omega(n)$ . While we do not obtain a full resolution of Question 1, we do show for the first time that  $\mathbf{UPP}^{\text{cc}}$  complexity can increase significantly under intersection.

Babai, Frankl and Simon [2] observed that there are two natural communication complexity analogs of the Turing machine class  $\mathbf{PP}$ , namely  $\mathbf{PP}^{\text{cc}}$  and  $\mathbf{UPP}^{\text{cc}}$ . It is well known [3] that  $\mathbf{PP}^{\text{cc}}$  is closed under intersection. Our work can be viewed as a first step towards showing that, in contrast,  $\mathbf{UPP}^{\text{cc}}$  is *not* closed under intersection.

► **Theorem 1.** *There is a function  $f(x, y): \{-1, 1\}^n \times \{-1, 1\}^n \rightarrow \{-1, 1\}$  such that  $\mathbf{UPP}^{\text{cc}}(f) = O(\log n)$ , yet  $\mathbf{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$ .*

In fact, for each fixed  $x \in \{-1, 1\}^n$ , the function  $f(x, y)$  from Theorem 1 simply outputs the majority of some subset of the bits of  $y$ . This yields the following corollary.

► **Corollary 2.** *Let  $\mathcal{C}$  be the concept class in which each concept is the intersection of two majorities on  $n$  bits. Then  $\mathcal{C}$  has dimension complexity  $n^{\Theta(\log n)}$ .*

Corollary 2 shows that the dimension complexity upper bound of Klivans et al. [16] is tight for intersections of two majorities, and new approaches will be needed to PAC learn this concept class in polynomial time. For context, we remark that learning intersections of majorities is a special case of the more general problem of learning intersections of many *halfspaces*.<sup>2</sup> The latter is a central and well-studied challenge in learning theory, as intersections of halfspaces are powerful enough to represent any convex set, and they contain many basic problems (like learning DNFs) as special cases. In contrast to the well-understood problem of learning a single halfspace, for which many efficient algorithms are known, no  $2^{o(n)}$ -time algorithm is known for PAC learning even the intersection of two halfspaces. There have been considerable efforts devoted to showing that learning intersections of halfspaces is a hard problem [18, 9, 15, 4], but these results apply only to intersections of many halfspaces, or make assumptions about the form of the output hypothesis of the learner. Our work can be seen as a new form of evidence that learning intersections of even two majorities is hard.

## 1.2 Our Techniques

$\mathbf{UPP}^{\text{cc}}$  has a *query complexity* analog, denoted  $\mathbf{UPP}^{\text{dt}}$  and defined as follows. A  $\mathbf{UPP}^{\text{dt}}$  algorithm is a randomized algorithm which on input  $x$ , queries bits of  $x$ , and must output  $f(x)$  with probability strictly greater than  $1/2$ ; the cost of the protocol is the number of bits of  $x$  queried. How  $\mathbf{UPP}^{\text{dt}}$  behaves under intersection is now well understood. More specifically, it is known [25] that there is a function  $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$  (in fact, a halfspace) such that  $\mathbf{UPP}^{\text{dt}}(f) = O(1)$ , yet  $\mathbf{UPP}^{\text{dt}}(f \wedge f) = \Theta(n)$ . Define the Majority function, which we denote by  $\text{MAJ}$ , to be  $-1$  if at least half of its input bits are  $-1$ . It is also known [26, 20] that  $\text{MAJ}$  satisfies  $\mathbf{UPP}^{\text{dt}}(\text{MAJ}) = O(1)$ , yet  $\mathbf{UPP}^{\text{dt}}(\text{MAJ} \wedge \text{MAJ}) = \Theta(\log n)$ . Our goal in this paper is, to the extent possible, to show that the  $\mathbf{UPP}^{\text{cc}}$  communication model behaves similarly to its query complexity analog.

<sup>2</sup> A halfspace is any function of the form  $\text{sgn}(\sum_{i=1}^n w_i \cdot x_i + w_0)$  for some real numbers  $w_0, \dots, w_n$ .

Over the course of the last decade, there has been considerable progress in proving *lifting theorems* [23, 12, 11]. These theorems seek to show that if a function  $f$  has large complexity in some query model  $\mathbf{C}$ , then for some “sufficiently complicated” function  $g$  on a “small” number of inputs, the composition  $f \circ g$  has large complexity in the associated communication model (ideally,  $\mathbf{C}^{\text{cc}}(f \circ g) \gtrsim \mathbf{C}^{\text{dt}}(f)$ ).

Unfortunately, a “generic” lifting theorem for  $\mathbf{UPP}$  complexity is not known. That is, it is not known how to take an arbitrary function  $f$  with high  $\mathbf{UPP}^{\text{dt}}$  complexity, and by composing it with a function  $g$  on a small number of inputs, yield a function with high  $\mathbf{UPP}^{\text{cc}}$  complexity.

However, as we now explain, some significant partial results have been shown in this direction. It is well-known that  $\mathbf{UPP}^{\text{dt}}(f)$  is equivalent to an approximation-theoretic notion called *threshold degree*, denoted  $\deg_{\pm}(f)$  (which we do not define here). The threshold degree of  $f$  can in turn be expressed as the value of a certain (exponentially large) linear program. Linear programming duality then implies that one can prove lower bounds on  $\deg_{\pm}(f)$  by exhibiting good solutions to the dual linear program. We refer to such dual solutions as *dual witnesses* for threshold degree. Sherstov [24] and Razborov and Sherstov [22] showed that if  $\deg_{\pm}(f)$  is large, and moreover this can be exhibited by a dual witness satisfying a certain *smoothness* condition, then there is a function  $g$  defined on a constant number of inputs such that  $f \circ g$  does have large  $\mathbf{UPP}^{\text{cc}}$  complexity. Several recent works [6, 5, 7, 28] have managed to prove new  $\mathbf{UPP}^{\text{cc}}$  lower bounds by constructing, for various functions  $f$ , smooth dual witnesses exhibiting the fact that  $\deg_{\pm}(f)$  is large.

Our key technical contribution is to bring this approach to bear on the function  $F(x, y) = \text{MAJ}(x) \wedge \text{MAJ}(y)$ . Specifically, we show that the (known) threshold degree lower bound  $\deg_{\pm}(F) \geq \Omega(\log n)$  can be exhibited by a smooth dual witness.

We do this as follows. Sherstov [26] showed that for any function  $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$ , the threshold degree of the function  $F = f \wedge f$  is characterized by the *rational approximate degree* of  $f$ , i.e., the least total degree of real polynomials  $p$  and  $q$  such that  $|f(x) - p(x)/q(x)| \leq 1/3$  for all  $x \in \{-1, 1\}^n$ . He then showed that the rational approximate degree of  $\text{MAJ}$  is  $\Omega(\log n)$ , thereby concluding that  $F(x, y)$  has threshold degree  $\Omega(\log n)$ .

From Sherstov’s arguments, one can derive a dual witness  $\psi$  for the fact that the rational approximate degree of  $\text{MAJ}$  is  $\Omega(\log n)$ , and then transform  $\psi$  into a dual witness  $\phi$  for the fact that  $F(x, y)$  has threshold degree  $\Omega(\log n)$ . Unfortunately, neither  $\psi$  nor  $\phi$  satisfies the type of smoothness condition required by Razborov and Sherstov’s machinery to yield  $\mathbf{UPP}^{\text{cc}}$  lower bounds.

The smoothness condition required for the Razborov-Sherstov machinery to work essentially states that the mass of the dual witness  $\psi$  has to be “relatively large” (a reasonably large fraction of what mass the uniform distribution would have placed) on a “large” set of inputs (the fraction of inputs which do not have large mass has to be small).

To construct a *smooth* dual witness  $\psi'$  for  $F$ , our primary technical contribution is to construct a *smooth* dual witness  $\phi'$  for the fact that the rational approximate degree of  $\text{MAJ}$  is  $\Omega(\log n)$ . We then apply a different transformation, due to Sherstov [27], of  $\phi'$  into a dual witness for the fact that the threshold degree of  $F$  is  $\Omega(\log n)$ , and we show that this transformation *preserves the smoothness* of  $\psi'$ .

In a nutshell, our smooth dual witness for  $\text{MAJ}$  is obtained in two steps: first we define for all inputs  $x$  whose Hamming weight lies in  $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$ , a dual witness  $\phi'_x$  that places a large mass on  $x$  and not too much mass on other points. Next, we define the final dual witness  $\phi'(x)$  to be a certain weighted average over  $x$  of all the dual witnesses thus obtained. The resulting mass on  $\phi'(x)$  for each  $x$  of Hamming weight

in  $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$  is large enough, and the fraction of inputs whose Hamming weight is not in  $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$  is small enough, to allow us to use the Razborov-Sherstov framework (Theorem 5) to prove the desired sign-rank lower bound on the pattern matrix of  $F$ .

## 2 Preliminaries

All logarithms in this paper are taken base 2. We use the notation  $\exp(x)$  to denote  $e^x$ , where  $e$  is Euler's number. Given any finite set  $X$  and any functions  $f, g : X \rightarrow \mathbb{R}$ , define  $\|f\|_1 := \sum_{x \in X} |f(x)|$  and  $\langle f, g \rangle := \sum_{x \in X} f(x)g(x)$ . We refer to  $\|f\|_1$  as the  $\ell_1$ -norm of  $f$ . For any  $x \in \{-1, 1\}^n$ , we use the notation  $|x|$  to denote the *Hamming weight* of  $x$ , which is the number of  $-1$ 's in the string  $x$ .

Paturi and Simon [21] showed the following equivalence between the sign-rank of a matrix and the  $\mathbf{UPP}^{cc}$  cost of its corresponding communication game.

► **Theorem 3.** *For any  $F : \{-1, 1\}^{2n} \times \{-1, 1\}^n \rightarrow \{-1, 1\}$ , let  $M_F$  denote its communication matrix, defined by  $M_F(x, y) = F(x, y)$ . Then,  $\mathbf{UPP}^{cc}(F) = \log \text{sr}(M_F) \pm O(1)$ .*

Let  $n, N$  be positive integers such that  $n$  divides  $N$ . Partition the set  $[N] := \{1, \dots, N\}$  into  $n$  disjoint blocks  $\{1, 2, \dots, N/n\}, \{N/n + 1, \dots, 2N/n\}, \dots, \{(n-1)N/n + 1, \dots, N\}$ . Define the set  $\mathcal{P}(N, n)$  to be the collection of subsets of  $[N]$  which contain exactly one element from each block. For  $x \in \{-1, 1\}^n$  and  $S \in \mathcal{P}(N, n)$ , let  $x|_S = (x_{s_1}, \dots, x_{s_n})$ , where  $s_1 < s_2 < \dots < s_n$  are the elements of  $S$ .

► **Definition 4 (Pattern matrix).** *For any function  $\phi : \{-1, 1\}^n \rightarrow \mathbb{R}$ , the  $(N, n, \phi)$ -pattern matrix  $M$  is defined as follows.*

$$M = [\phi(x|_S) \oplus w]_{x \in \{-1, 1\}^n, (S, w) \in \mathcal{P}(N, n) \times \{-1, 1\}^n}.$$

Note that  $M$  is a  $2^N \times (N/n)^n 2^n$  matrix.

In a breakthrough result, Forster [10] proved that an upper bound on the spectral norm of a sign matrix implies a lower bound on its sign-rank. Razborov and Sherstov [22] established a generalization of Forster's theorem [10] that can be used to prove sign-rank lower bounds for pattern matrices. Specifically, we require the following result, implicit in their work [22, Theorem 1.1].

► **Theorem 5 (Implicit in [22]).** *Let  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$  be any Boolean function and  $\alpha > 1$  be a real number. Suppose there exists a function  $\phi : \{-1, 1\}^n \rightarrow \mathbb{R}$  satisfying the following conditions.*

- $\sum_{x \in \{-1, 1\}^n} |\phi(x)| = 1$ .
- For all polynomials  $p$  of degree at most  $d$ ,  $\sum_{x \in \{-1, 1\}^n} \phi(x)p(x) = 0$ .
- $f(x) \cdot \phi(x) \geq 0 \ \forall x \in \{-1, 1\}^n$ .
- $|\phi(x)| \geq \gamma$  for all but a  $\Delta$  fraction of inputs  $x \in \{-1, 1\}^n$ .

Then, the sign-rank of the  $(N, n, f)$ -pattern matrix  $M$  can be bounded below as

$$\text{sr}(M) \geq \frac{\gamma}{\frac{1}{2^n} \left(\frac{n}{N}\right)^{d/2} + \gamma\Delta}.$$

We require the following well-known combinatorial identity.

► **Claim 6.** For every polynomial  $p$  of degree less than  $2n$ , we have  $\sum_{t=-n}^n (-1)^t \binom{2n}{n+t} p(t) = 0$ .

Recall from Section 1.2 that the rational  $\epsilon$ -approximate degree of  $f$  is the least degree of two polynomials  $p$  and  $q$  such that  $|f(x) - p(x)/q(x)| \leq \epsilon$  for all  $x$  in the domain of  $f$ . Sherstov [27, Theorem 6.9] showed that a dual witness to the rational approximate degree of any function  $f$  can be converted to a threshold degree dual witness for  $\text{OR}_n \circ f$ . Implicit in his theorem is the fact that a *smooth* dual witness to the rational approximate degree of  $f$  can be converted to a *smooth* dual witness for the threshold degree of  $\text{OR}_n \circ f$ . More precisely, the following result is established by the proof of [27, Theorem 6.9].

► **Theorem 7** (Sherstov [27]). *Let  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$  be any function. Let  $F$  denote  $\text{OR}_t \circ f : \{-1, 1\}^{nt} \rightarrow \{-1, 1\}$ , and  $\delta > \epsilon > 0$  be any real numbers.*

*Suppose there exist functions  $\psi_0, \psi_1 : \{-1, 1\}^n \rightarrow \mathbb{R}$  that are not identically 0 and satisfy the following properties:*

$$f(x) = 1 \implies \psi_0(x) \geq \delta |\psi_1(x)|, \quad (1)$$

$$f(x) = -1 \implies \psi_1(x) \geq \delta |\psi_0(x)|, \quad (2)$$

$$\deg(p) < d \implies \langle \psi_0, p \rangle = 0 \text{ and } \langle \psi_1, p \rangle = 0. \quad (3)$$

*Then there exist functions  $A, B : \{-1, 1\}^{nt} \rightarrow \mathbb{R}$  such that  $\Psi = \frac{1}{\delta}A - \frac{1}{\epsilon}B$  satisfies the following properties.*

$$\deg(p) \leq \min\{\lfloor \epsilon^2 t \rfloor d, d\} \implies \langle \Psi, p \rangle = 0. \quad (4)$$

$$F(x) \cdot \Psi(x_1, \dots, x_t) \geq (\delta - \epsilon)^{2t} \prod_{i=1}^t |\psi_0(x_i)| \text{ for all } x \in \{-1, 1\}^{nt}. \quad (5)$$

$$|A(x_1, \dots, x_t)| \leq \prod_{i=1}^t |\psi_0(x_i)| \text{ for all } x = (x_1, \dots, x_t) \in \{-1, 1\}^{nt}. \quad (6)$$

$$|B(x_1, \dots, x_t)| \leq \prod_{i:f(x_i)=0} |\psi_0(x_i)| \cdot \prod_{i:f(x_i)=1} \delta \psi_1(x_i) + \prod_{i=1}^t (|\psi_0(x_i)| - \delta \psi_1(x_i))$$

for all  $x = (x_1, \dots, x_t) \in \{-1, 1\}^{nt}$ . (7)

### 3 A Smooth Dual Witness for Majority

Our main technical contribution in this paper is captured in Theorem 8 below. This theorem constructs a *smooth* dual witness  $R$  for the hardness of rationally approximating the sign function on  $\{0, \pm 1, \dots, \pm n\}$ . We defer the proof until Section 4.

► **Theorem 8.** *Let  $1 \leq d \leq \frac{1}{3} \log n$  and let  $n$  be odd. There exists a function  $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  such that*

$$\sum_{t=-n}^n |R(t)| = 1. \quad (8)$$

■ *For  $\delta = \exp(-18/(n^{1/(6d)}))$  and every  $t = 1, 2, \dots, n$ ,*

$$R(t) \geq \delta |R(-t)|. \quad (9)$$

■ *If  $p : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  is any polynomial of degree less than  $d - 2$ , then*

$$\langle R, p \rangle = 0. \quad (10)$$

■ For every  $t \in \{0, \pm 1, \pm 2, \dots, \pm \lfloor n^{2/3} \rfloor\}$  we have

$$|R(t)| \geq \Omega\left(\frac{1}{n^{20}}\right). \quad (11)$$

The following theorem shows how to convert the (univariate) function  $R$  from Theorem 8 into a dual witness for the (multivariate) MAJ function.

► **Theorem 9.** *Let  $1 \leq d \leq \frac{1}{3} \log n$  and let  $n$  be odd. Let  $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  be any function obtained in Theorem 8. Then, the multivariate polynomial  $R' : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$  defined by  $R'(x) = R(n - |x|) / \binom{2n}{|x|}$  satisfies the following properties.*

■  $\|R'\|_1 = 1.$  (12)  
 ■ For  $\delta = \exp(-18/(n^{1/(6d)}))$  and every  $t = 1, 2, \dots, n$ ,

$$R'(x) \geq \delta |R'(y)| \quad (13)$$

for any  $x, y \in \{-1, 1\}^{2n}$  such that  $|x| = n - t, |y| = n + t$ .

■ For any polynomial  $p$  of degree at most  $d - 2$ ,

$$\langle R', p \rangle = 0. \quad (14)$$

■ For all  $x \in \{-1, 1\}^{2n}$  such that  $n - \lfloor n^{2/3} \rfloor \leq |x| \leq n + \lfloor n^{2/3} \rfloor$ ,

$$|R'(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right). \quad (15)$$

**Proof.** To establish Equation (12), observe:

$$\begin{aligned} \|R'\|_1 &= \sum_{x \in \{-1, 1\}^{2n}} |R'(x)| = \sum_{t=0}^{2n} \left( \sum_{x \in \{-1, 1\}^{2n} : |x|=t} |R'(x)| \right) \\ &= \sum_{t=0}^{2n} \binom{2n}{t} |R(n-t)| / \binom{2n}{t} = \sum_{t=-n}^n |R(t)| = 1, \end{aligned}$$

where the last equality follows from Equation (8). Equation (13) follows directly from Equation (9) and the definition of  $R'$ .

To establish Equation (14), consider any polynomial  $p : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$  of degree at most  $d - 2$ . For any permutation  $\sigma \in S_{2n}$ , define the polynomial  $p_\sigma$  by  $p_\sigma(x_1, \dots, x_{2n}) = p(x_{\sigma(1)}, \dots, x_{\sigma(2n)})$ . Note that, since  $R'$  is symmetric,  $\langle R', p_\sigma \rangle = \langle R', p \rangle$  for all  $\sigma \in S_{2n}$ . Define  $q = \mathbb{E}_{\sigma \in S_{2n}} [p_\sigma]$ . Note that  $q$  is symmetric and  $\langle R', p \rangle = \langle R', q \rangle$ . It is a well-known fact (cf. [19]) that  $q$  can be written as a polynomial  $q'$  of degree at most  $d - 2$  in the variable  $\sum_{i=1}^{2n} x_i$ , and so can  $R'$ . Hence,  $\langle R', p \rangle = \langle R', q \rangle = \sum_{t=0}^{2n} \binom{2n}{t} \frac{R(n-t)}{\binom{2n}{t}} \cdot q'(t) = 0$ , where the final equality holds by Equation (10).

To establish Equation (15), observe that by Equation (11) and the definition of  $R'$ , we have that for all  $x \in \{-1, 1\}^{2n}$  such that  $|x| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$ ,  $|R'(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot \binom{2n}{|x|}}\right) \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right)$ . ◀

We are ready to derive a lower bound on the sign-rank of the  $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$ -pattern matrix.

► **Theorem 10.** *The  $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$ -pattern matrix  $M$  satisfies  $\text{sr}(M) \geq n^{\Omega(\log n)}$ .*

**Proof.** Let  $F$  denote the function  $\text{OR}_2 \circ \text{MAJ}_{2n}$  in this proof. Set  $d = \log n/100$  and consider the function  $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  obtained via Theorem 8. Define the function  $R' : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  by  $R'(t) = R(-t)$ . Define the functions  $\psi_0, \psi_1 : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$  by  $\psi_1(x) = R(n - |x|)/\binom{2n}{|x|}$ , and  $\psi_0(x) = R'(n - |x|)/\binom{2n}{|x|}$ . We now verify that  $\psi_0, \psi_1$  satisfy the conditions in Theorem 7 for  $\delta = \exp(-18/(n^{1/(6d)})) = \exp(-18/n^{100/6 \log n}) = \exp(-18/2^{100/6}) > 0.99$ . Set  $\varepsilon = \delta \cdot c$ , where  $c > 0$  is a constant such that  $0.98 > \delta \cdot c > 1/\sqrt{2}$ .

- By the definitions of  $\psi_0, \psi_1$  and Equation (13), Properties (1) and (2) in the statement of Theorem 7 are satisfied.
- Equation (14) implies that  $\langle \psi_0, p \rangle = \langle \psi_1, p \rangle = 0$  for any polynomial  $p$  of degree at most  $d - 2$ , and hence Property (3) is satisfied.

Moreover, Equation (15) implies that  $|\psi_0(x)|, |\psi_1(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right)$  for all  $x \in \{-1, 1\}^{2n}$  such that  $n - \lfloor n^{2/3} \rfloor \leq |x| \leq n + \lfloor n^{2/3} \rfloor$ , and Equation (12) implies  $\|\psi_0\|_1 = \|\psi_1\|_1 = 1$ . Theorem 7 now implies the existence of a function  $\Psi$  satisfying the following properties.

- By Equation (4),  $\deg(p) < \min\{\lfloor 2\varepsilon^2 \rfloor \cdot ((\log n)/100 - 2), (\log n)/100 - 2\} \implies \langle \Psi, p \rangle = 0$ . Since  $\varepsilon > 1/\sqrt{2}$ , this implies that

$$\deg(p) < (\log n)/100 - 2 \implies \langle \Psi, p \rangle = 0.$$

- By Equation (5),  $\Psi(x) \cdot F(x) \geq 0$  for all  $x \in \{-1, 1\}^{2n} \times \{-1, 1\}^{2n}$ .
- We now note that the functions  $A$  and  $B$  obtained in Theorem 7 have  $\ell_1$ -norm at most a constant. Since  $\|\psi_0\|_1 = \|\psi_1\|_1 = 1$ , we use Equation (6) to conclude that

$$\sum_{x_1, x_2 \in \{-1, 1\}^{2n} \times \{-1, 1\}^{2n}} |A(x_1, x_2)| \leq \sum_{x_1 \in \{-1, 1\}^{2n}} |\psi_0(x_1)| \cdot \sum_{x_2 \in \{-1, 1\}^{2n}} |\psi_0(x_2)| = 1.$$

By Equation (7), we have

$$\begin{aligned} \sum_{x_1, x_2 \in \{-1, 1\}^{2n}} |B(x_1, x_2)| &\leq \max\{\|\psi_0\|_1, \delta\|\psi_1\|_1\}^2 + \|\psi_0\|_1^2 + \delta\|\psi_0\|_1\|\psi_1\|_1 + \\ &\quad \delta^2\|\psi_1\|_1^2, \end{aligned}$$

which is at most a constant, since  $\delta = O(1)$ .

Combined with the fact that  $\varepsilon$  is a constant, we conclude  $\|\Psi\|_1 \leq \frac{1}{\delta}\|A\|_1 + \frac{1}{\varepsilon}\|B\|_1 \leq O(1)$ .

- By Equation (5),  $F(x) \cdot \Psi(x_1, x_2) \geq (\delta - \varepsilon)^4 |\psi_0(x_1)| \cdot |\psi_0(x_2)| \forall x \in \{-1, 1\}^{4n}$ . This implies that for  $|x_1|, |x_2| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$ ,

$$|\Psi(x_1, x_2)| \geq \Omega\left(\frac{1}{n^{40} \cdot 2^{4n}}\right),$$

since  $\delta - \varepsilon = \Omega(1)$ .

- By a standard Chernoff bound, the number of inputs in  $\{-1, 1\}^{2n} \times \{-1, 1\}^{2n}$  such that  $|x_1|, |x_2| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$  is at least  $(1 - 2\exp(-n^{1/3}/3)) \cdot 2^{4n}$ .

Plugging  $f = \text{OR}_2 \circ \text{MAJ}_{2n}$  and  $\phi = \frac{\Psi}{\|\Psi\|_1}$  into Theorem 5, we conclude that the sign-rank of the  $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$  pattern matrix  $M$  is bounded below as

$$\text{sr}(M) \geq \Omega\left(\frac{\frac{1}{n^{40}} \cdot \frac{1}{2^{4n}}}{\left(\frac{1}{n^{(\log n/200)-1}} \cdot \frac{1}{2^{4n}}\right) + \left(\frac{1}{n^{40}} \cdot \frac{1}{2^{4n}} \cdot 2\exp(-n^{1/3}/3)\right)}\right) \geq n^{\Omega(\log n)}.$$

We are now ready to prove Theorem 1.



**Proof of Theorem 1.** Note that the function  $\text{AND} \circ \text{MAJ}(x) = \overline{\text{OR} \circ \text{MAJ}(\bar{x})}$ . Consider the dual witness  $\phi = \frac{\Psi}{\|\Psi\|_1}$  obtained for the threshold degree of  $\text{OR}_2 \circ \text{MAJ}_{2n}$  in the previous proof. Note that the function  $\phi'$  defined by  $\phi'(x) = -\phi(\bar{x})$  acts as a dual witness for the threshold degree of  $\text{AND}_2 \circ \text{MAJ}_{2n}$ , and satisfies all the conditions in Theorem 5 with the same parameters as in the proof of Theorem 10. Proceeding in exactly the same way as in the previous proof, we conclude that sign-rank of the  $(4n^2, 4n, \text{AND}_2 \circ \text{MAJ}_{2n})$  pattern matrix  $M'$  is bounded below as

$$\text{sr}(M') \geq n^{\Omega(\log n)}. \quad (16)$$

Denote by  $f$  the communication game corresponding to the  $(2n^2, 2n, \text{MAJ}_{2n})$  pattern matrix. For completeness, we now sketch a standard  $\mathbf{UPP}^{\text{cc}}$  protocol of cost  $O(\log n)$  for  $f$ . Note that Alice holds  $2n^2$  input bits, and Bob holds a  $(2n \cdot \log n)$ -bit string indicating the “relevant bits” in each block of Alice’s input and a  $2n$ -bit string  $w$ . Bob sends Alice the index of a uniformly random relevant bit using  $\log(2n^2)$  bits of communication. Alice responds with her value  $b$  of that input bit, and Bob outputs  $b \oplus w_i$ . It is easy to check that this is a valid  $\mathbf{UPP}^{\text{cc}}$  protocol, and it has cost  $O(\log n)$ .

One can verify by the definition of pattern matrices (Definition 4) that the communication game corresponding to the  $(4n^2, 4n, \text{AND}_2 \circ \text{MAJ}_{2n})$  pattern matrix  $M'$  equals  $f \wedge f$ . By Theorem 3 and Equation (16), we obtain that

$$\mathbf{UPP}(f \wedge f) = \Theta(\log \text{sr}(M')) = \Omega(\log^2 n).$$

As mentioned in Section 1, the result of Klivans et al. [16] implies that  $\text{sr}(M') = n^{O(\log n)}$ . Thus, the function  $f$  satisfies  $\mathbf{UPP}^{\text{cc}}(f) = O(\log n)$ , but  $\mathbf{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$ . ◀

Corollary 2 follows immediately from the previous proof and the definition of pattern matrices.

## 4 Proof of Theorem 8

The rest of this paper is dedicated towards proving Theorem 8. Before proving the theorem, we describe the main auxiliary construction and prove some preliminary facts about it.

Let  $\Delta = \lfloor n^{1/(3d)} \rfloor \geq 2$ . Fix any  $u \in \{1, \dots, \lfloor n^{2/3} \rfloor - 1, \lfloor n^{2/3} \rfloor\}$ . Define the set

$$S_u = \{\pm u, \pm u\Delta, \pm u\Delta^2, \dots, \pm u\Delta^{d-1}\}.$$

Define the polynomial  $r_u : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$  by

$$r_u(t) = \frac{1}{(2n)!} \prod_{i=0}^{d-1} \left( t - \left( u\Delta^i \sqrt{\Delta} \right) \right) \prod_{s \notin S_u} (t - s).$$

Since  $n$  is odd, notice that  $\text{sgn}(r_u(t)) = (-1)^t$ , for  $t \in \{u, u\Delta, u\Delta^2, \dots, u\Delta^{d-1}\}$ , and  $r_u(t) = 0$  for  $t \notin S_u$ .

Define

$$p_u(t) = \binom{2n}{n+t} r_u(t) = \begin{cases} (-1)^{n-t} \cdot \frac{\prod_{i=0}^{d-1} \left( t - \left( u\Delta^i \sqrt{\Delta} \right) \right)}{\prod_{\substack{s \in S_u \\ s \neq t}} (t - s)} & \text{if } t \in S_u \\ 0 & \text{otherwise.} \end{cases}$$

### 30:10 Sign-Rank Can Increase Under Intersection

The following claim tells us that for any  $u \in \{1, \dots, \lfloor n^{2/3} \rfloor\}$ , the function  $p_u$  places a reasonably large mass on input  $-u$ .

▷ Claim 11.

$$|p_u(-u)| \geq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2}.$$

Proof. We calculate

$$\begin{aligned} |p_u(-u)| &= \frac{u(\sqrt{\Delta} + 1)}{2u} \cdot \prod_{i=1}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} + 1)}{u^2(\Delta^i + 1)(\Delta^i - 1)} \\ &\quad \text{(pairing terms corresponding to } u\Delta^i \text{ and } -u\Delta^i) \\ &= \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \prod_{i=1}^{d-1} \frac{\Delta^{i+\frac{1}{2}} + 1}{\Delta^{2i} - 1} \geq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{(d-1)/2} \cdot \prod_{i=1}^{d-1} \frac{\Delta^i}{\Delta^{2i}} \\ &= \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2}. \end{aligned} \quad \triangleleft$$

The next claim tells us that the mass placed by  $p_u$  on other points in its support is small.

▷ Claim 12. For every  $j = 1, 2, \dots, d-1$ ,

$$|p_u(-u\Delta^j)| \leq e^4 \cdot \Delta^{-(j^2-3j-2)/2} \cdot \left( \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2} \right).$$

Proof. We calculate

$$\begin{aligned} |p_u(-u\Delta^j)| &= \frac{u(\Delta^j \sqrt{\Delta} + \Delta^j)}{2u\Delta^j} \cdot \prod_{i=0}^{j-1} \frac{u(\Delta^i \sqrt{\Delta} + \Delta^j)}{u^2(\Delta^i + \Delta^j)(\Delta^j - \Delta^i)} \cdot \prod_{i=j+1}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} + \Delta^j)}{u^2(\Delta^i + \Delta^j)(\Delta^i - \Delta^j)} \\ &\quad \text{(pairing terms corresponding to } u\Delta^i \text{ and } -u\Delta^i) \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \prod_{i=0}^{j-1} \frac{\sqrt{\Delta}}{\Delta^j - \Delta^i} \cdot \prod_{i=j+1}^{d-1} \frac{\sqrt{\Delta}}{\Delta^i - \Delta^j} \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \prod_{i=0}^{j-1} \frac{\Delta^{j-i} \cdot \Delta^{-j}}{\Delta^{j-i} - 1} \cdot \prod_{i=j+1}^{d-1} \frac{\Delta^{-i} \cdot \Delta^{i-j}}{\Delta^{i-j} - 1} \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \prod_{i=0}^{j-1} \Delta^{-j} \cdot \prod_{i=j+1}^{d-1} \Delta^{-i} \cdot \left( \prod_{k=1}^{\infty} \frac{\Delta^k}{\Delta^k - 1} \right)^2 \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \Delta^{-j^2 - (d(d-1) - (j+2)(j+1))/2} \cdot \exp \left( 2 \sum_{k=1}^{\infty} \frac{1}{\Delta^k - 1} \right) \\ &\quad \text{(since } 1 + x \leq e^x \text{ for all } x \in \mathbb{R}) \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(j^2-3j-2)/2} \cdot \Delta^{-(d-1)^2/2} \cdot \exp \left( 4 \sum_{k=1}^{\infty} \frac{1}{\Delta^k} \right) \quad \text{(since } \Delta \geq 2) \\ &\leq e^4 \cdot \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(j^2-3j-2)/2} \cdot \Delta^{-(d-1)^2/2}. \quad \text{(again using } \Delta \geq 2) \end{aligned}$$

◁

The following claim tells us that for each  $u$  and  $j$ , the masses placed by  $r_u$  (and hence  $p_u$ ) on  $u\Delta^j$  and  $-u\Delta^j$  are comparable.

▷ **Claim 13.** For every  $j = 0, 1, \dots, d-1$ , we have

$$|r_u(-u\Delta^j)| \geq |r_u(u\Delta^j)| \geq \exp(-18/\sqrt{\Delta})|r_u(-u\Delta^j)|$$

$$\text{and } |p_u(-u\Delta^j)| \geq |p_u(u\Delta^j)| \geq \exp(-18/\sqrt{\Delta})|p_u(-u\Delta^j)|.$$

**Proof.** We may write the ratio

$$\frac{|p_u(u\Delta^j)|}{|p_u(-u\Delta^j)|} = \frac{|r_u(u\Delta^j)|}{|r_u(-u\Delta^j)|} = \prod_{i=0}^{j-1} \frac{u(\Delta^j - \Delta^i \sqrt{\Delta})}{u(\Delta^j + \Delta^i \sqrt{\Delta})} \cdot \prod_{i=j}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} - \Delta^j)}{u(\Delta^j + \Delta^i \sqrt{\Delta})}.$$

This is a product of terms smaller than 1, yielding the first inequality. For the second, we follow Sherstov's argument [26, Theorem 5.3] and note that this product is at least

$$\begin{aligned} \left( \prod_{i=1}^{\infty} \frac{\Delta^{i/2} - 1}{\Delta^{i/2} + 1} \right)^2 &\geq \exp \left( -5 \sum_{i=1}^{\infty} \frac{1}{\Delta^{i/2}} \right) \\ &\quad \text{since } (a-1)/(a+1) > \exp(-2.5/a) \text{ for } a \geq \sqrt{2} \\ &= \exp \left( \frac{-5}{\sqrt{\Delta}} \sum_{i=0}^{\infty} \frac{1}{\Delta^{i/2}} \right) \geq \exp \left( \frac{-5}{\sqrt{\Delta}} \cdot \frac{1}{1 - 1/\sqrt{2}} \right) \quad \text{since } \Delta \geq 2 \\ &\geq \exp \left( -\frac{18}{\sqrt{\Delta}} \right). \quad \triangleleft \end{aligned}$$

Putting the three claims together, we obtain the following conclusion, which states that the mass placed by  $p_u$  on  $-u$  and  $u$  is a relatively large fraction of its  $\ell_1$ -norm.

► **Lemma 14.**  $|p_u(-u)| \geq \|p_u\|_1 / (8\Delta^2 e^4)$  and  $|p_u(-u)| \geq |p_u(u)| \geq \frac{\exp(-18/\sqrt{\Delta}-4)}{8\Delta^2} \cdot \|p_u\|_1$ .

**Proof.** We bound the ratio

$$\begin{aligned} \frac{\|p_u\|_1}{|p_u(-u)|} &\leq 2 \sum_{j=0}^{d-1} \frac{|p_u(-u\Delta^j)|}{|p_u(-u)|} && \text{by the first inequality in Claim 13} \\ &\leq 2 \left( 1 + \sum_{j=0}^{d-1} e^4 \Delta^{-(j^2-3j-2)/2} \right) && \text{by Claims 11 and 12} \\ &\leq 2 + 2e^4 \left( \sum_{j=0}^3 \Delta^{-(j^2-3j-2)/2} + \sum_{j=4}^{\infty} \Delta^{-(j^2-3j-2)/2} \right) \\ &\leq 8\Delta^2 \cdot e^4 \cdot \sum_{k=1}^{\infty} \Delta^{-k} \leq 8 \cdot \Delta^2 \cdot e^4. && \text{since } \Delta \geq 2 \end{aligned}$$

By the above and the second inequality in Claim 13,

$$|p_u(u)| \geq \exp(-18/\sqrt{\Delta})|p_u(-u)| \geq \frac{\exp(-18/\sqrt{\Delta}-4)}{8\Delta^2} \cdot \|p_u\|_1. \quad \blacktriangleleft$$

We are now ready to prove Theorem 8.

**Proof of Theorem 8.** Define the function  $P(t) = \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(t)}{\|p_u\|_1}$ . We claim that the function  $R: \{0, \pm 1, \dots, \pm n\} \rightarrow \{-1, 1\}$  defined by  $R(t) = \frac{(-1)^t P(t)}{\|P\|_1}$  satisfies the conditions in Theorem 8.

■ Clearly,  $\sum_{t=-n}^n |R(t)| = 1$ , i.e.,  $R$  satisfies Equation (8).

### 30:12 Sign-Rank Can Increase Under Intersection

- By Claim 13, for every  $u = 1, \dots, \lfloor n^{2/3} \rfloor$  and every  $t = 1, \dots, n$ ,  $(-1)^t p_u(t) \geq \delta |p_u(-t)|$  for  $\delta = \exp(-18/\sqrt{\Delta}) = \exp(-18/n^{1/6d})$ . Therefore, for all such  $t$  we also have  $(-1)^t P(t) \geq \delta |P(t)|$ , which implies  $R(t) \geq \delta |R(-t)|$  for every  $t = 1, 2, \dots, n$ .
- We have

$$R(t) = \frac{(-1)^t P(t)}{\|P\|_1} = \frac{(-1)^t}{\|P\|} \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(t)}{\|p_u\|_1} = \frac{(-1)^t}{\|P\|_1} \binom{2n}{n+t} \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{r_u(t)}{\|p_u\|_1}.$$

Since each  $r_u$  is a polynomial of degree at most  $(2n+1) - d$ , Claim 6 implies that for any polynomial  $p$  of degree at most  $d-2$ ,  $\langle R, p \rangle = 0$ .

- It now remains to verify the smoothness condition. Fix a point  $v \in \{1, \dots, \lfloor n^{2/3} \rfloor\}$ . Since  $\text{sgn}(p_u(v)) = (-1)^v$  for all  $u$  and for all  $v > 0$ , we have that

$$\begin{aligned} \frac{|P(v)|}{\|P\|_1} &\geq v^{20} \cdot \frac{|p_v(v)| \cdot \|p_v\|_1^{-1}}{\sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20}} \geq \frac{\exp(-18/\sqrt{\Delta}-4)/8\Delta^2}{\lfloor n^{2/3} \rfloor \cdot (\lfloor n^{2/3} \rfloor)^{20}} && \text{by Lemma 14} \\ &\geq \frac{\exp(-18/\sqrt{2}-4)}{8n^{15}} \geq \frac{e^{-15}}{8n^{15}}. && \text{since } n^{1/3} \geq \Delta = \lfloor n^{1/3d} \rfloor \geq 2 \end{aligned}$$

If  $v < 0$ , the argument needs some more care because we do not have the guarantee that  $\text{sgn}(p_u(v)) = (-1)^v$ . The large mass placed by  $p_{-v}$  on the point  $v$  plays a crucial role.

$$\begin{aligned} |P(v)| &\geq \frac{(-v)^{20} \cdot |p_{-v}(v)|}{\|p_{-v}\|_1} - \sum_{\substack{u=1 \\ u \neq v}}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(-v)}{\|p_u\|_1} \\ &\geq \frac{(-v)^{20}}{8\Delta^2 e^4} - \sum_{j=1}^{\lfloor \log_{\Delta}(-v) \rfloor} (-v\Delta^{-j})^{20} \cdot \frac{p_{-v\Delta^{-j}}(v)}{\|p_{-v\Delta^{-j}}\|_1} \\ &\quad \text{by Lemma 14, the definition of } p_u \text{ and its support} \\ &\geq (-v)^{20} \left[ \frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{-20j} \cdot \Delta^{(-j^2+3j+2)/2} \right] && \text{by Claims 11 and 12} \\ &= (-v)^{20} \left[ \frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{(-j^2-37j+2)/2} \right] \geq (-v)^{20} \left[ \frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{-18j} \right] \\ &\geq (-v)^{20} \left[ \frac{1}{8\Delta^2 e^4} - \frac{e^4}{\Delta^{17}} \right] = (-v)^{20} \left[ \frac{\Delta^{15} - 8e^8}{8\Delta^{17} e^4} \right] \geq \frac{20}{\Delta^{17}} \geq \frac{20}{n^6} \\ &\quad \text{since } n^{1/3} \geq \Delta \geq 2 \text{ and } (-v) \geq 1 \end{aligned}$$

Thus, we have that for  $v < 0$ ,

$$\frac{|P(v)|}{\|P\|_1} \geq \frac{20}{n^6 \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20}} \geq \frac{20}{n^6 \lfloor n^{2/3} \rfloor \cdot (\lfloor n^{2/3} \rfloor)^{20}} \geq \frac{20}{n^{20}}. \quad \blacktriangleleft$$

## 5 Conclusion

We have exhibited a communication problem  $f$  with  $\mathbf{UPP}^{\text{cc}}(f) = O(\log n)$ , and  $\mathbf{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$ . This is the first result showing that  $\mathbf{UPP}$  communication complexity can increase by more than a constant factor under intersection. As a consequence, we have concluded that the dimension-complexity-based quasipolynomial time PAC learning algorithm of [16] for learning intersections of polylogarithmically many majorities is optimal. That is, new learning algorithms not based on dimension complexity will be required to learn this class in polynomial time.

A glaring open question left by our work is whether the class of problems with polylogarithmic  $\text{UPP}^{\text{cc}}$  complexity is closed under intersection. Our results represent an important first step in this direction. It would also be very interesting to extend our result that dimension-complexity-based algorithms cannot PAC learn intersections of two majorities in polynomial time, to rule out an even larger class of learning algorithms. Specifically, it would be very interesting to show that no algorithm working in the important *statistical query* model [14] can learn this concept class in polynomial time.

---

## References

---

- 1 Andris Ambainis, Andrew M Childs, Ben W Reichardt, Robert Špalek, and Shengyu Zhang. Any AND-OR formula of size  $N$  can be evaluated in time  $N^{1/2+o(1)}$  on a quantum computer. *SIAM Journal on Computing*, 39(6):2513–2530, 2010.
- 2 László Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory (preliminary version). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*, pages 337–347, 1986. doi:10.1109/SFCS.1986.15.
- 3 Richard Beigel, Nick Reingold, and Daniel A. Spielman.  $PP$  Is Closed under Intersection. *J. Comput. Syst. Sci.*, 50(2):191–202, 1995. doi:10.1006/jcss.1995.1017.
- 4 Arnab Bhattacharyya, Suprovat Ghoshal, and Rishi Saket. Hardness of Learning Noisy Halfspaces using Polynomial Thresholds. In *Conference On Learning Theory, COLT 2018, Stockholm, Sweden, 6-9 July 2018.*, pages 876–917, 2018. URL: <http://proceedings.mlr.press/v75/bhattacharyya18a.html>.
- 5 Adam Boulund, Lijie Chen, Dhiraj Holden, Justin Thaler, and Prashant Nalini Vasudevan. On the Power of Statistical Zero Knowledge. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 708–719, 2017. doi:10.1109/FOCS.2017.71.
- 6 Mark Bun and Justin Thaler. Improved Bounds on the Sign-Rank of  $AC^0$ . In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 37:1–37:14, 2016. doi:10.4230/LIPIcs.ICALP.2016.37.
- 7 Mark Bun and Justin Thaler. The Large-Error Approximate Degree of  $AC^0$ . *Electronic Colloquium on Computational Complexity (ECCC)*, 25:143, 2018. URL: <https://eccc.weizmann.ac.il/report/2018/143>.
- 8 Arkadev Chattopadhyay and Nikhil S. Mande. A Short List of Equalities Induces Large Sign Rank. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 47–58, 2018. doi:10.1109/FOCS.2018.00014.
- 9 Vitaly Feldman, Parikshit Gopalan, Subhash Khot, and Ashok Kumar Ponnuswami. New results for learning noisy parities and halfspaces. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pages 563–574. IEEE, 2006.
- 10 Jürgen Forster. A linear lower bound on the unbounded error probabilistic communication complexity. *J. Comput. Syst. Sci.*, 65(4):612–625, 2002. doi:10.1016/S0022-0000(02)00019-3.
- 11 Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-Communication Lifting for  $P^{NP}$ . In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 12:1–12:16, 2017. doi:10.4230/LIPIcs.CCC.2017.12.
- 12 Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-Communication Lifting for  $BPP$ . In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 132–143, 2017. doi:10.1109/FOCS.2017.21.
- 13 Mika Göös, Toniann Pitassi, and Thomas Watson. The Landscape of Communication Complexity Classes. *Computational Complexity*, 27(2):245–304, 2018. doi:10.1007/s00037-018-0166-6.
- 14 Michael Kearns. Efficient noise-tolerant learning from statistical queries. *Journal of the ACM (JACM)*, 45(6):983–1006, 1998.

- 15 Subhash Khot and Rishi Saket. On the hardness of learning intersections of two halfspaces. *Journal of Computer and System Sciences*, 77(1):129–141, 2011.
- 16 Adam R. Klivans, Ryan O’Donnell, and Rocco A. Servedio. Learning intersections and thresholds of halfspaces. *J. Comput. Syst. Sci.*, 68(4):808–840, 2004. doi:10.1016/j.jcss.2003.11.002.
- 17 Adam R Klivans and Rocco A Servedio. Learning DNF in time  $2^{O(n^{1/3})}$ . *Journal of Computer and System Sciences*, 68(2):303–318, 2004.
- 18 Adam R Klivans and Alexander A Sherstov. Cryptographic hardness for learning intersections of halfspaces. *Journal of Computer and System Sciences*, 75(1):2–12, 2009.
- 19 Marvin Minsky and Seymour Papert. *Perceptrons*. MIT Press, 1969.
- 20 Ryan O’Donnell and Rocco A Servedio. New degree bounds for polynomial threshold functions. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 325–334. ACM, 2003.
- 21 Ramamohan Paturi and Janos Simon. Probabilistic Communication Complexity. *J. Comput. Syst. Sci.*, 33(1):106–123, 1986. doi:10.1016/0022-0000(86)90046-2.
- 22 Alexander A. Razborov and Alexander A. Sherstov. The Sign-Rank of  $AC^0$ . *SIAM J. Comput.*, 39(5):1833–1855, 2010. doi:10.1137/080744037.
- 23 Alexander A. Sherstov. The Pattern Matrix Method. *SIAM J. Comput.*, 40(6):1969–2000, 2011. doi:10.1137/080733644.
- 24 Alexander A Sherstov. The unbounded-error communication complexity of symmetric functions. *Combinatorica*, 31(5):583–614, 2011.
- 25 Alexander A. Sherstov. Optimal bounds for sign-representing the intersection of two halfspaces by polynomials. *Combinatorica*, 33(1):73–96, 2013. doi:10.1007/s00493-013-2759-7.
- 26 Alexander A. Sherstov. The Intersection of Two Halfspaces Has High Threshold Degree. *SIAM J. Comput.*, 42(6):2329–2374, 2013. doi:10.1137/100785260.
- 27 Alexander A Sherstov. Breaking the Minsky–Papert Barrier for Constant-Depth Circuits. *SIAM Journal on Computing*, 47(5):1809–1857, 2018.
- 28 Alexander A. Sherstov and Pei Wu. Near-Optimal Lower Bounds on the Threshold Degree and Sign-Rank of  $AC^0$ . *CoRR*, abs/1901.00988, 2019. To appear in STOC 2019. arXiv:1901.00988.